Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A machine-implemented method comprising:

producing a first authentication message comprising:

authentication data encrypted with a first key;

and a data structure comprising the first key, wherein the data structure is encrypted with a second key;

generating in a mobile device a registration request message to have a ~~first network device~~ home agent associated with a ~~first~~ home network deliver datagrams destined for a home address associated with ~~a~~ the mobile device on the ~~first~~ home network to a second address on a second, different network; and

embedding the authentication message in the registration request message.

2. (Original) The method of claim 1 wherein the authentication data comprises a timestamp.

3. (Original) The method of claim 1 wherein the second key is known to the first network device and unknown to the mobile node.

4. (Original) The method of claim 1 wherein the authentication message comprises a Kerberos Application Request.

5. (Original) The method of claim 1 wherein the data structure comprises a Kerberos ticket.

6. (Original) The method of claim 1 further comprising generating a second authentication message.

7. (Original) The method of claim 6, wherein generating a second authentication message comprises: generating a hash of the request message using the first key.

8. (Currently Amended) The method of claim 6 further comprising: transmitting the request message and second authentication message to the home agent ~~first network device~~.

9. (Currently Amended) The method of claim 8 further comprising: receiving the request message and second authentication message by ~~a device~~ the home agent on the home network; and decrypting the data structure using the second key to obtain the first key.

10. (Original) The method of claim 9 further comprising: verifying the second authentication message using the first key.

11. (Original) The method of claim 9 further comprising generating a third key.

12. (Original) The method of claim 9 further comprising generating key material, wherein the key material-may be supplied to a function to generate a third key.

13. (Canceled)

14. (Original) The method of claim 11 further comprising: forming a reply authentication message comprising the third key encrypted with the first key.

15. (Original) The method of claim 14 wherein the reply authentication message comprises a Kerberos Application Reply message.

16. (Original) The method of claim 14 further comprising: forming a reply message that includes the reply authentication message.

17. (Original) The method of claim 16 wherein the reply message comprises a Registration Reply message.

18. (Original) The method of claim 16 further comprising: generating a third authentication message; and transmitting the reply message and third authentication message to the mobile node.

19. (Original) The method of claim 18 wherein generating a third authentication message comprises: generating a hash of the reply authentication message using the first key.

20. (Currently Amended) A machine-implemented method comprising:

receiving at a ~~first device~~ home agent associated with a home network an authentication message ~~and~~ embedded in a registration request message to reroute datagrams destined for a first address of a mobile device associated with the home network to a second address not associated with the home network, wherein the request message comprises:

a data structure that includes a first key encrypted with a second key; and

determining if the authentication message is valid.

21. (Original) The method of claim 20 further comprising: generating a third key if the authentication message is determined to be valid.

22. (Original) The method of claim 20 further comprising: generating key material if the authentication message is determined to be valid, wherein the key material may be supplied to a function known to the first device and the mobile device to produce a third key.

23. (Original) The method of claim 20 wherein the authentication message comprises a hash of the request message, wherein the hash is computed using the first key.

24. (Canceled)

25. (Original) The method of claim 23, wherein determining if the authentication message is valid comprises: computing a hash of the request message using the first key; and comparing the computed hash to the authentication message.

26. (Original) The method of claim 25 further comprising: decrypting the data structure using the second key to obtain the first key.

27. (Currently Amended) The method of claim 21 further comprising: receiving a reply message from the home agent ~~first device~~ by the mobile device, wherein the reply message includes the third key.

28. (Currently Amended) The method of claim 27 further comprising:

forming a second request message to have datagrams destined for a first address of a mobile device associated with the home network to a third address not associated with the home network;

forming a second authentication message using the third key; and transmitting the second request message and second authentication message to the home agent ~~first device~~.

29. (Currently Amended) A computer program product residing on a computer readable medium having instructions stored thereon that, when executed by the processor, cause that processor to:

form an authentication message comprising:

authentication data encrypted with a first key; and

the first key encrypted with a second key;

generate a registration request message requesting that datagrams destined for a first Internet Protocol address of a mobile device be routed to a second Internet Protocol address; and

include the authentication request message in the request message.

30. (Original) The computer program product of claim 29 wherein the authentication message comprises a Kerberos Application Request message.

31. (Original) The computer program product of claim 29 further comprising instructions to generate a hash of the request message using the first key to form a second authentication message.

32. (Currently Amended) The computer program product of claim 29 further comprising instructions to:

receive a reply message from ~~the first device~~ a home agent by the mobile device, wherein the reply message includes a third key;

form a second authentication message using the third key;

transmit a second request message to have datagrams destined for a first address of a mobile device associated with ~~the~~ a home network to a third address not associated with the home network, wherein the second authentication message is included in the second request message.

33. (Currently Amended) A computer program product residing on a computer readable medium having instructions stored thereon that, when executed by the processor, cause that processor to:

extract an authentication message from a registration request message requesting that datagrams destined for a first Internet Protocol address of a mobile device be routed to a second Internet Protocol address, wherein the authentication message comprises:

authentication data encrypted with a first key; and

a data structure comprising the first key, and encrypted with a second key;

verify the authentication data; and

if the authentication data is valid, then generating a third key.

34. (Original) The computer program product of claim 33 further comprising instructions that cause the processor to:

form a reply message that includes the third key; and

transmit the reply message to a device associated with the request message.

35. (Original) The computer program product of claim 33 further comprising instructions that cause the processor to: store the encryption key.

36. (Canceled)

37. (Currently Amended) A system comprising:

a ~~first network device~~ home agent associated with a first network; and

a second network device associated with the first network, the second network device ~~capable of~~ operable to:

~~producing~~ produce an authentication message including a data structure comprising the first key with the data structure encrypted with a second key;

~~generating~~ generate a registration request message to have the ~~first network device~~ home agent deliver datagrams destined for a home address associated with the second device on the first network to a second address on a second, different network; and

~~including~~ include the authentication message within the request message.

38. (Currently Amended) The system of claim 37 wherein the second network device is further ~~capable of forming~~ operable to form a second authentication message by computing a hash of the request message using the first key.

39. (Currently Amended) The system of claim 38 wherein the ~~first network device~~ home agent is ~~capable of receiving~~ operable to receive the request message and ~~generating~~ generate a key if the second authentication message is valid.

40. (Currently Amended) The system of claim 37 wherein the ~~first network device~~ home agent is a router.

41. (Original) The system of claim 37 wherein the second network device is a laptop computer.

42. (Currently Amended) The system of claim 37 further comprising: a third device ~~capable of producing~~ operable to produce the first key and the data structure encrypted with the second key.

43. (Currently Amended) A system comprising:

a router associated with a ~~first~~ home network and comprising an input port for receiving datagrams and a switch fabric for determining destination of datagrams; and

a processor ~~capable of~~ operable to:

~~reading~~ read a registration request message to reroute datagrams destined for a first address of a mobile device associated with the ~~first~~ home network to a second address associated with a second, different network, wherein the request message includes a data structure comprising a first key unknown to the processor encrypted with a second key that is known to the processor[[,]];

~~verifying~~ verify an authentication message associated with the request message wherein the authentication message comprises a hashed version of the request message computed using the first key; and

if the authentication message is valid, then ~~generating~~ generate a third key.

44. (Currently Amended) The system of claim 43, wherein the processor is further ~~capable of~~ operable to: ~~encrypting~~ encrypt the third key.

45. (Currently Amended) The system of claim 44, wherein the processor is further ~~capable of~~ operable to:

~~forming~~ form a reply message, wherein the reply message includes the encrypted third key; and

~~forming~~ form a reply authentication message.

46. (Currently Amended) The ~~method~~ system of claim 45 wherein the reply authentication message comprises a hashed version of the reply message.

47. (Currently Amended) The ~~method~~ system of claim 45 ~~further comprising~~ wherein the processor is further operable to:

~~transmitting~~ transmit the reply message and the reply authentication message to the mobile device at the second address.